PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

OAV

(51) Internationale Patentklassifikation 6 : H04L 9/08

A1

(11) Internationale Veröffentlichungsnummer: **WO 95/34969**

(43) Internationales Veröffentlichungsdatum: 21. December 1995 (21.12.95)

(21) Internationales Aktenzeichen: PCT/DE95/00738

(22) Internationales Anmeldedatum: 30. Mai 1995 (30.05.95)

(30) Prioritätsdaten:
P 44 20 967.3 16. Juni 1994 (16.06.94) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: ESD VERMÖGENSVERWALTUNGSGESELLSCHAFT MBH [DE/DE]; Brienner Strasse 10, D-80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: BUGOVICS, Jozsef [HU/DE]; Kreuzstrasse 11, D-06886 Lutherstadt Wittenberg (DE).

(74) Anwalt: HAUSSINGEN, Peter; Franz-Heymann-Strasse 70, D-06526 Sangerhausen (DE).

(81) Bestimmungsstaaten: AU, BR, CN, CZ, JP, KR, NO, PL, RU, SG, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

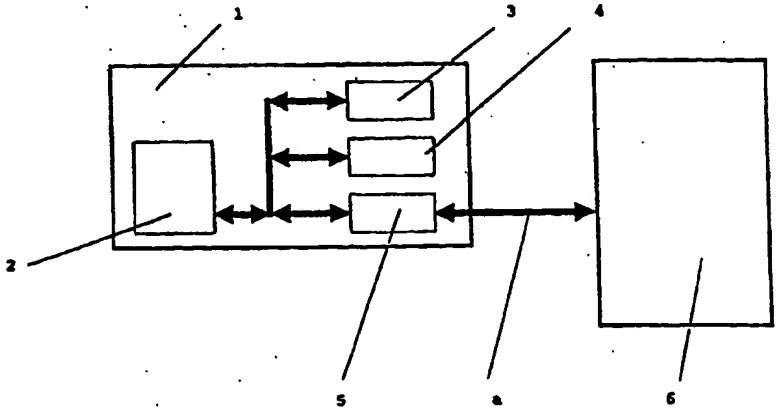
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: DEVICE FOR DECODING DIGITAL DATA AND METHOD OF ENCRYPTING AND DECODING SUCH DATA USING THE DEVICE

(54) Bezeichnung: ENTSCHLÜSSELUNGSEINRICHTUNG VON DIGITALEN INFORMATIONEN UND VERFAHREN ZUR DURCHFÜHRUNG DER VER- UND ENTSCHLÜSSELUNG DERSELBEN

(57) Abstract

The aim of the invention is to develop a device and a method by means of which keys with frequently changing encryption algorithms can be encrypted, whereby certain keys must be accessible to certain persons and the distribution of the keys and their protection from decoding is ensured. This aim is achieved by virtue of the fact that the decoding device consists of an integrated circuit (1) associated with a central processing unit (2), an internal non-readable volatile random-access memory (3) used as working memory and an internal non-readable non-volatile read-only memory (4) plus an interface (5), each decoding device differing from every other by the content of the ROM (4) and being partly integrated in an integrated circuit (1) and that the interface (5) is located between the central processing unit (2) and the personal computer (6) and connected, together with the central processing unit (2), to the personal computer (6) by a data path (a).



(57) Zusammenfassung

Die Erfindung betrifft eine Entschlüsselungseinrichtung von digitalen Informationen und Verfahren zur Durchführung der Ver- und Entschlüsselung derselben. Die Aufgabe ist es, eine Vorrichtung und ein Verfahren zu entwickeln, nach denen die Schlüssel mit öfter wechselnden Verschlüsselungsalgorithmen verschlüsselt werden sollen, wobei bestimmte Schlüssel für bestimmte Personen verfügbar sein müssen und die Verteilung der Schlüssel und der Schutz vor Entschlüsselung gegeben ist. Erfindungsgemäß wird die Aufgabe dadurch gelöst, daß die Entschlüsselungseinrichtung aus einem integrierten Schaltkreis (1), dem ein Zentralprozessor CPU (2), ein interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM (3) als Arbeitsspeicher und ein interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM (4) und ein Interface (5) zugeordnet sind, indem sich jede Entschlüsselungseinrichtung von jeder weiteren unterscheidet durch den Inhalt des internen nichtflüchtigen Speichers mit wahlfreiem Zugriff ROM (4) und teilweise in einem integrierten Schaltkreis (1) integriert ist und daß das Interface (5) zwischen dem Zentralprozessor CPU (2) und dem Personalcomputer (6) angeordnet ist und mit dem Zentralprozessor CPU (2) mit dem Datenpfad (a) verbunden sind.

Entschlüsselungseinrichtung von digitalen Informationen und Verfahren zur Durchführung der Ver- und Entschlüsselung derselben

Die Erfindung betrifft eine Entschlüsselungseinrichtung von digitalen Informationen und das Verfahren zur Durchführung der Ver- und Entschlüsselung derselben, indem die Entschlüsselungseinrichtung Berechtigten den Zugriff gewährt und Unberechtigte vom Zugriff ausschließt.

Digitale Informationen werden in immer größerem Maßstab über ungesicherte Verteilungskanäle versandt. Diese Informationen sollen aber sicherstellen, daß nur die berechtigte Person den Schlüssel erhält und die Information entschlüsseln kann. Die Schlüsselübergabe muß so gestaltet werden, daß es nur berechtigten Personen möglich ist, die Schlüssel zu nutzen und die Weitergabe unmöglich ist.

In der Druckschrift US 84/01856 wird ein Ver-/Entschlüsselungsapparat (EDU) beschrieben. Diese Erfindung verfolgt das Ziel, den sicheren Schlüsselaustausch über ungesicherte Datenleitungen (z. B. Telefonleitungen) zu ermöglichen. Jede EDU enthält einen Zentralprozessor (CPU), Speicher mit wahlfreiem Zugriff (ROM), in welchem Schlüsselaustauschschlüssel (KEK) gespeichert sind und einen „data-encryption standard“ (DES) Koprozessor; alles in einem Keramikmodul eingebettet, um die Untersuchung der Befehlsabarbeitung unmöglich zu machen. Weiterhin enthält jede EDU einen Spezialschaltkreis, welcher es der CPU ermöglicht, verschlüsselte Befehle abzuarbeiten. Bei Aufnahme einer Verbindung zwischen zwei EDU's wählt jede EDU einen Teilschlüssel. Dieser Teilschlüssel wird verschlüsselt an die Gegenstelle übertragen und geprüft. Danach werden beide Teilschlüssel zum sogenannten Sessionkey zusammengesetzt. Mit diesem Sessionkey wird dann die Information verschlüsselt und übertragen.

Ein Nachteil dieser Erfindung ist, daß eine Verbindung in beiden Richtungen nötig ist, um den Schlüssel auszutauschen. Dies ist bei dieser Methode auch nötig, da beide EDU's jeweils einen Teil des Schlüssels erzeugen, der dann zur jeweils anderen EDU übertragen und zum vollständigen Schlüssel zusammengesetzt wird.

Weiterhin ist es auf diese Weise möglich, Informationen an Empfängergruppen mit der gleichen Verschlüsselung zu versenden, da für jede Verbindung zweier EDU's ein anderer Schlüssel generiert wird.

Die Druckschrift EP 0266748 beschreibt einen Koprozessor mit Entschlüsselungseigenschaften und nichtauslesbaren Schlüsseltafeln. Diese Schlüsseltafeln werden mit einem Übergabemodul in den Koprozessor übertragen. Bei der Übertragung der Schlüsseltafel für die ein bestimmtes Programm in den Koprozessor wird das Übergabemodul entwertet. Dadurch wird ein mehrfaches Übertragen der Schlüsseltafel in mehrere Koprozessoren verhindert. Damit ist es dann möglich, Programme, zu denen die Schlüsseltafeln in den Koprozessor übertragen wurden, zu entschlüsseln.

Der Nachteil dieser Erfindung ist jedoch, daß die Übergabe eines Transfertokens in einem speziellen Speicher (Hardware-Übergabemodul) zu erfolgen hat, der dann bei der Benutzung entwertet wird. Dies bringt natürlich Handlingprobleme mit sich. Dieses Modul muß an den Endkunden weitergeleitet werden. Es ist dann auch keine nochmalige Entschlüsselung der Information möglich, da das Übergabemodul entwertet wurde. Weiterhin ist keine Schlüsselübergabe über elektronische Medien möglich.

Um die oben genannten Nachteile des Standes der Technik zur Verteilung von Informationen zu beheben, ist es Aufgabe der Erfindung, ein Verfahren zu schaffen, mit dem Informationen bedienerfreundlich an mehrere Empfänger verteilt werden können, sowie einen geringen verwaltungstechnischen Aufwand zur Informationsverschlüsselung hat.

Es besteht also die Notwendigkeit, ein Verfahren zu finden, mit dem es möglich ist, Schlüssel sicher zu verteilen und die Übertragung dieser gegen Erkunden zu schützen.

Weiterhin ist es notwendig, daß es selbst dem Besitzer eines Entschlüsselungsgerätes nicht möglich ist, einen Schlüssel weiterzugeben.

Um diese Forderung zu erfüllen, ist es möglich, die Schlüssel in irgendeiner Weise zu verschlüsseln.

Die modernen Möglichkeiten zum Brechen eines Verschlüsselungsalgorithmus beruhen auf dem Vorhandensein von sogenannten Plaintexten (unverschlüsselte Information) und der dazugehörigen Ciphertexte (verschlüsselte Information). Um Blocksysteme, wie z. B. den DEA zu brechen, muß die Menge dieser Texte sehr groß sein. Dies ist notwendig, um solche Methoden, wie die differentielle Cryptoanalyse von Biham und Shamir, durchzuführen. Diese Methode ist der beste zur Zeit bestehende Angriff auf Bockverschlüsselsysteme wie den DEA (beschrieben in Eli Biham und Ali Shamir „Differential Cryptoanalysis of DES-like Cryptosysteme" in Journal of Cryptology vol. 4 pp 3-72, 1991).

Ein Erkunden des Verschlüsselungsverfahrens des Schlüssels soll aber weitgehend erschwert werden.

Es ist also nötig, die Menge der Dritten zur Verfügung stehenden Plain-/Ciphertexte möglichst gering zu halten, was besonders bei der Schlüsselübergabe nötig ist.

Dies erreicht man dadurch, daß die Schlüssel mit öfter wechselnden Verschlüsselungsalgorithmen verschlüsselt werden. Dritte, welche die Schlüssel entschlüsseln wollen, müssen dann jedesmal einen neuen „Knackalgorithmus" entwickeln, wenn das Verschlüsselungsverfahren gewechselt wird.

Weiterhin ist es damit möglich, bestimmte Schlüssel nur für bestimmte Personen und auch Personenkreise verfügbar zu machen, indem diesen das Entschlüsselungsverfahren für Schlüssel zugänglich gemacht werden.

Es ist ebenfalls nötig, einen Spezialprozessor als Teil dieses Verfahrens zu schaffen, der die Verteilung der Schlüssel ermöglicht, sowie den Schutz von Entschlüsselungsverfahren der Schlüssel vor Weitergabe preiswert und sicher realisiert.

Ebenfalls notwendig ist es, daß es auch den rechtmäßigen Empfängern eines Entschlüsselungsverfahrens für Schlüssel nicht möglich ist, diese weiterzugeben.

Erfindungsgemäß wird diese Aufgabe durch die im Patentanspruch 1 und Patentanspruch 2 angegebenen Merkmale gelöst. Bevorzugte Weiterbildungen ergaben sich aus den Unteransprüchen.

Die Erfindung wird nachstehend anhand der Figur 1, die die Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen für Schlüssel zeigt und dem Verfahren zur Durchführung der Ver- und Entschlüsselung von digitalen Informationen, dargestellt.

Die in Figur 1 dargestellte Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen von Schlüsseln wird zur Verdeutlichung anhand eines Einsatzes in mehreren Personalcomputern gezeigt, wobei digitale Informationen an ausgewählte Besitzer von Entschlüsselungseinrichtungen gesandt werden.

Dabei besteht die dargestellte Entschlüsselungseinrichtung aus einem -integrierten Schaltkreis-1, dem ein -Zentralprozessor CPU-2, ein -interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM-3 als Arbeitsspeicher und ein -interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM-4 [in welchem zwei interne nichtauslesbare Entschlüsselungsalgorithmen (EI und EA) gespeichert sind] und ein Interface 5 zugeordnet sind, welches zwischen dem -Zentralprozessor CPU-2 und dem Personalcomputer 6 angeordnet ist und mit dem Personalcomputer 6 mit dem Datenpfad a verbunden ist, und teilweise in einem -integrierten Schaltkreis-1 integriert ist.

Die Übertragung eines Entschlüsselungsalgorithmus für Schlüssel an eine Entschlüsselungseinrichtung geschieht wie folgt:

Der Verteiler wählt einen Verschlüsselungsalgorithmus EEU. Dieser sei zum Verschlüsseln der später übertragenen Schlüssel gedacht. Dieser Verschlüsselungsalgorithmus muß natürlich geheim gehalten werden und muß weiterhin sicher genug sein, um Sicherheit bei der Verschlüsselung von Schlüsseln zu bieten. Dafür würden sich z. B. verschiedene Abarten des DES (z. B. mit verschiedenen S-Boxen) oder andere Verschlüsselungsverfahren eignen.

Nun wird der zum Verschlüsselungsalgorithmus EEU passende Entschlüsselungsalgorithmus EE zum unleserlichen Algorithmus EEV verschlüsselt.

Nun kann jeder Benutzer einer Entschlüsselungseinrichtung, der einen Schlüssel erhalten will, sich bei der Verteilerstelle melden. Dies kann z. B. verbal (auch über Telefon), schriftlich oder elektronisch erfolgen. Anhand der öffentlichen Seriennummer der Entschlüsselungseinrichtung muß er sich identifizieren. Da diese Seriennummer nur einmal vergeben wird, ist es der Entschlüsselungseinrichtung möglich, die Entschlüsselungseinrichtung und deren Besitzer eindeutig zu identifizieren. Die Verteilungsstelle kann nun darüber entscheiden, ob der Empfänger berechtigt ist, den Entschlüsselungsalgorithmus zu empfangen. Das kann auch von einer Bezahlung abhängen.

Wenn dies geklärt ist, wird der verschlüsselte Entschlüsselungsalgorithmus EEV zum Benutzer der Entschlüsselungseinrichtung übertragen und dort in der Entschlüsselungseinrichtung zum Algorithmus EE entschlüsselt.

Nun ist es möglich, Schlüssel, die mit dem Verschlüsselungsalgorithmus EEU verschlüsselt wurden, zu entschlüsseln.

Dies soll nun an einem Ausführungsbeispiel dargestellt werden.

Es soll eine Menge von digitalen Informationen an ausgewählte Kunden versandt werden. Dabei soll allen die gesamte Information übertragen werden, aber nicht alle Kunden sollen den Zugriff auf alle Informationen haben. Eine preiswerte Realisierung dafür stellt z. B. die Verteilung dieser Informationen per CD-ROM dar. Diese Datenträger sind in großen Stückzahlen preiswert zu produzieren und können sehr große Datenmengen speichern. Es liegt also nahe, alle Informationen verschlüsselt auf einer CD-ROM unterzubringen, sie an alle Kunden zu senden und dann nur noch die Berechtigung an die Kunden zu verteilen, damit sie die Information nutzen können. Diese Berechtigung soll mit dieser Erfindung folgendermaßen übertragen werden.

Es seien nun die CD`s an alle Kunden verteilt. Weiterhin sei Kunde A im Besitz der Entschlüsselungseinrichtung mit der Seriennummer SN=1.

Nun soll der Kunde A die Information B erhalten. Diese Information liegt auf der CD-ROM mit dem zum gewöhnlichen internen Entschlüsselungsalgorithmus EA passenden Verschlüsselungsalgorithmus EAU unter Nutzung des Schlüssels K nach

$$NV := EAU(NE, K)$$

verschlüsselt.

Jetzt muß der Kunde A noch den Schlüssel erhalten.

Dazu wird beim Verteiler der Informationen die Übergabe des Schlüssels an die Entschlüsselungseinrichtung vorbereitet. Es wählt der Verteiler der Informationen einen Verschlüsselungsalgorithmus EEU, welcher dann zur Verschlüsselung des später zu übertragenden Schlüssels genutzt werden soll. Dieser Verschlüsselungsalgorithmus wird nie offen, sondern nur in verschlüsselter Form übertragen.

Der Hersteller der Entschlüsselungseinrichtung / die Verteilungsstelle der Informationen verfügt in einer Datenbank über die internen Entschlüsselungsalgorithmen EI und auch die zugehörigen Verschlüsselungsalgorithmen EIU aller an Kunden ausgegebenen Entschlüsselungseinrichtungen.

Es sei EI1, der interne Entschlüsselungsalgorithmus EI der Entschlüsselungseinrichtung (mit der internen Seriennummer SN=1) beim Kunden A. Weiterhin sei EI1U, der ebenfalls nur dem Hersteller der Entschlüsselungseinrichtung bekannte Verschlüsselungsalgorithmus passend zu EI1.

Nun wird der, der Entschlüsselungseinrichtung zu übertragende Schlüssel K verschlüsselt. Dies erfolgt in der Art, daß dieser mit dem zu übertragenden Entschlüsselungsalgorithmus EE passenden Verschlüsselungsalgorithmus EEU zum unleserlichen Schlüssel S nach folgender Formel verschlüsselt wird:

$$S := EEU(K).$$

Dieser verschlüsselte Schlüssel S wird der Entschlüsselungseinrichtung übertragen.

Um diesen Schlüssel zu entschlüsseln, benötigt die Entschlüsselungseinrichtung beim Kunden A natürlich ebenfalls den Entschlüsselungsalgorithmus EE. Da dieser aber geheimgehalten werden muß, wird er in verschlüsselter Form übertragen.

Dies erfolgt in der Art, daß der Entschlüsselungsalgorithmus EE mit dem zum internen Entschlüsselungsalgorithmus EI der Entschlüsselungseinrichtung passenden Verschlüsselungsalgorithmus EIU zum unleserlichen Algorithmus EEV nach folgender Formel verschlüsselt wird:

$$EEV := EI1U(EE).$$

Dieser verschlüsselte Algorithmus EEV wird der Entschlüsselungseinrichtung beim Kunden A übertragen.

Dies kann z. B. verbal (auch über Telefon), schriftlich oder elektronisch erfolgen.

Der übermittelte verschlüsselte Algorithmus und der verschlüsselte Schlüssel sind relativ kurz. Damit ist ein Knacken des internen Entschlüsselungsalgorithmus der Entschlüsselungseinrichtung EI schwer möglich. Wie oben gezeigt, müssen für ein Brechen der Verschlüsselung viele Plain- und Ciphertexte vorhanden sein, um erfolgversprechende Knackalgorithmen verwenden zu können. Dies ist aber in diesem Fall wegen der geringen Menge der übermittelten Informationen schwer möglich.

Nun wird beim Empfänger das Entschlüsselungsgerät funktionstüchtig gemacht.

Der Ablauf beim Einschalten der Versorungsspannung oder nach einer Unterbrechnung der Abarbeitung ist folgender:

Der -Zentralprozessor CPU-2 führt mit dem -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-4 und dem -internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM-3 einen Selbsttest durch. Dies könnte z. B. durch eine Prüfsummenbildung geschehen.

Der Entschlüsselungsalgorithmus in verschlüsselter Form EEV wird nun beim Kunden, vom Benutzer der Entschlüsselungseinrichtung, in den Personalcomputer 6 eingegeben oder in anderer Form eingelesen.

Nun erfolgt das Einlesen des verschlüsselten Entschlüsselungsalgorithmus EEV in die Entschlüsselungseinrichtung über das Interface 5.

Als nächstes wird mit Hilfe des im -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-4 gespeicherten Entschlüsselungs-

algorithmus EI der verschlüsselt vorliegende Entschlüsselungsalgorithmus EEV mit dem internen Entschlüsselungsverfahren EI entschlüsselt. Dies geschieht in der Weise, daß der -Zentralprozessor CPU-2 die im -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-4 gespeicherten Anweisungen des Entschlüsselungsalgorithmus EI ausführt und den verschlüsselten Entschlüsselungsalgorithmus EEV folgendermaßen entschlüsselt:

EE:= EI1 (EEV).

Bei diesem Verfahren entsteht wieder, da der interne Entschlüsselungsalgorithmus EI1 mit dem Verschlüsselungsalgorithmus EIU1 zusammenpaßt mit dem der Entschlüsselungsalgorithmus EE verschlüsselt wurde, der ursprüngliche Entschlüsselungsalgorithmus EE.

Dieser wird im -internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM-3 abgespeichert und ist somit nicht von außen erkundbar. Damit ist es nicht möglich, den Entschlüsselungsalgorithmus weiterzugeben, da er in verschlüsselter Form wertlos ist und in unverschlüsselter Form nicht vorliegt.

Nun ist die Entschlüsselungseinrichtung einsatzbereit und es ist nun die Möglichkeit gegeben, den Schlüssel K zu berechnen.

Die Entschlüsselung eines Schlüssels, der an den Kunden in verschlüsselter Form übertragen wurde, erfolgt folgendermaßen:

Die CPU lädt über das Interface 5 den Schlüssel S.

Nun wird mit Hilfe der nichtauslesbaren Schlüsselberechnungsfunktion EE in der Entschlüsselungseinrichtung der Schlüssel berechnet nach:

K:= EE(S).

Dieser Schlüssel K ist nie außerhalb der Entschlüsselungseinrichtung zu finden und auch nicht erkundbar. Damit ist es niemandem möglich, diesen weiterzugeben.

Nun wird die Information von der CD-ROM vom Interface 6 geladen.

Als nächstes wird sie mit dem vom -Zentralprozessor CPU-2 mit dem gewöhnlichen Entschlüsselungsalgorithmus der Entschlüsselungseinrichtung EA unter Nutzung des Schlüssels K entschlüsselt:

$$NE := EA(NV, K).$$

Danach wird die entschlüsselte Information NE von dem -Zentralprozessor CPU-2 über das Interface 5 ausgegeben und steht dem Kunden zur Verfügung.

Damit gelingt es, den Zugriff auf die verschlüsselten Informationen flexibel zu gestalten. Weiterhin besteht die Möglichkeit, bestimmten Gruppen von Empfängern oder einzelnen Empfängern, Teile der Information einer CD-ROM zugänglich zu machen, ohne, daß es diesen möglich ist, die Schlüssel weiterzugeben. Damit gelingt es, Schlüssel mit verschiedenen Verschlüsselungsalgorithmen zu verschlüsseln und mit verschiedenen Entschlüsselungseinrichtungen zu entschlüsseln, ohne daß der Entschlüsselungsalgorithmus bekannt werden muß oder vorher schon in der Entschlüsselungseinrichtung vorliegt.

Weiterhin ist der übertragene Entschlüsselungsalgorithmus für Schlüssel weder weitergebbar noch erkundbar, da er individuell für jedes Entschlüsselungsgerät verschlüsselt übertragen wird, dort nichtauslesbar gespeichert und nur zum internen Gebrauch des Entschlüsselungsgerätes mit der entsprechenden Seriennummer verfügbar ist. Es wird damit die Möglichkeit geschaffen, auch Entschlüsselungseinrichtungen vom Informationsempfang auszuschließen.

Verwendete Bezugszeichen

1	-integrierter Schaltkreis-
2	-Zentralprozessor CPU-
3	-interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM-
4	-interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM-
5	Interface
6	Personalcomputer
a	Datenpfad

Verwendete Abkürzungen

CPU = Zentralprozessor

DEA = data encryption standard

EA = Entschlüsselungsalgorithmus intern zur Entschlüsselung von Informationen

EAU = Verschlüsselungsalgorithmus beim Verteiler der Informationen zur Verschlüsselung der Informationen passend zu EA

EI = Entschlüsselungsalgorithmus intern zur Entschlüsselung von übertragenen Entschlüsselungsalgorithmen

EI1 = Entschlüsselungsalgorithmus intern für die Entschlüsselungseinrichtung mit der Seriennummer SN=1

EIU = zum internen Entschlüsselungsalgorithmus EI passender Verschlüsselungsalgorithmus

EI1U = zum internen Entschlüsselungsalgorithmus EI1 passender Verschlüsselungsalgorithmus für die Entschlüsselungseinrichtung mit der Seriennummer SN=1

EE = Entschlüsselungsalgorithmus zur Entschlüsselung von verschlüsselten Schlüsseln

EEV = verschlüsselter Entschlüsselungsalgorithmus

EEU = Verschlüsselungsalgorithmus passend zu EE

NE = nichtverschlüsselte oder entschlüsselte Information

NV = verschlüsselte Information

Schlüssel K = Schlüssel zur Entschlüsselung von Nachrichten

Schlüssel S = mit dem Verschlüsselungsalgorithmus EEU verschlüsselter Schlüssel zur Entschlüsselung von Nachrichten

(:=) = ergibt sich aus

Patentansprüche

1. Entschlüsselungseinrichtung von digitalen Informationen, dadurch gekennzeichnet, daß vom Verteiler des Entschlüsselungsalgorithmus dieser mit einem Verschlüsselungsalgorithmus (EIU) verschlüsselt wird, welcher dem Entschlüsselungsalgorithmus (EI) entspricht, der in der jeweiligen empfangenden Entschlüsselungseinheit intern vorhanden ist und daß der Entschlüsselungsalgorithmus (EI) der Öffentlichkeit nicht zugänglich und auch nicht erkundbar ist, daß der Nutzer der Entschlüsselungseinrichtung den verschlüsselten Entschlüsselungsalgorithmus in die Entschlüsselungseinrichtung eingibt und dieser innerhalb der Entschlüsselungseinrichtung entschlüsselt wird, daß die Entschlüsselungseinrichtung aus einem -integrierten Schaltkreis-(1), dem ein -Zentralprozessor CPU-(2), ein -interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM-(3) als Arbeitsspeicher und ein -interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM-(4) und ein Interface (5) zugeordnet sind, indem sich jede Entschlüsselungseinrichtung von jeder weiteren unterscheidet durch den Inhalt des -internen nichtflüchtigen Speichers mit wahlfreiem Zugriff ROM-(4) und teilweise in einem -integrierten Schaltkreis-(1) integriert ist und daß das Interface (5) zwischen dem -Zentralprozessor CPU-(2) und dem Personalcomputer (6) angeordnet ist und mit dem -Zentralprozessor CPU-(2) mit dem Datenpfad (a) verbunden sind.

2. Entschlüsselungseinrichtung von digitalen Informationen und Verfahren zur Durchführung der Ver- und Entschlüsselung derselben dadurch gekennzeichnet, daß im

1. Schritt

vom Verteiler des Entschlüsselungsalgorithmus dieser mit einem, nur dem Hersteller der Entschlüsselungseinrichtung bekannten Verschlüsselungsalgorithmus (EIU), welcher dem Entschlüsselungsalgorithmus (EI) in der Entschlüsselungseinheit entspricht, wie folgt verschlüsselt wird:

EEV:= EIV (EE)

und dieser verschlüsselte Algorithmus (EEV) der Entschlüsselungseinrichtung übertragen wird, wonach im

2. Schritt

die Entschlüsselungseinrichtung, mit dem -Zentralprozessor CPU-(2) mit dem -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-(4) einen Selbsttest durchführt, und das Einlesen des verschlüsselten Entschlüsselungsalgorithmus (EEV) in das Entschlüsselungsgerät über das Interface (5) erfolgt und nun mit Hilfe des im -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-(4) gespeicherten Entschlüsselungsalgorithmus (EI) der verschlüsselt vorliegende Entschlüsselungsalgorithmus (EEV) mit dem internen Entschlüsselungsverfahren (EI) nach

EE:= EI (EEV)

entschlüsselt wird, wobei bei diesem Verfahren wieder der ursprüngliche Entschlüsselungsalgorithmus (EE) entsteht, welcher im

3. Schritt

im -internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM-(3) abgespeichert, und somit nicht von außen erkundbar ist, womit die Entschlüsselungseinrichtung mit dem Entschlüsselungsalgorithmus (EE) einsatzbereit ist und die Entschlüsselung eines Schlüssels (S) im

4. Schritt

folgendermaßen erfolgt, daß die CPU über das Interface (5) den Schlüssel (S) lädt und der Schlüssel von dem -Zentralprozessor CPU-(2) mit dem Entschlüsselungsalgorithmus (EE) nach

K:=EE (S)

entschlüsselt wird und der Schlüssel damit für die Entschlüsselung der Information zur Verfügung steht und im

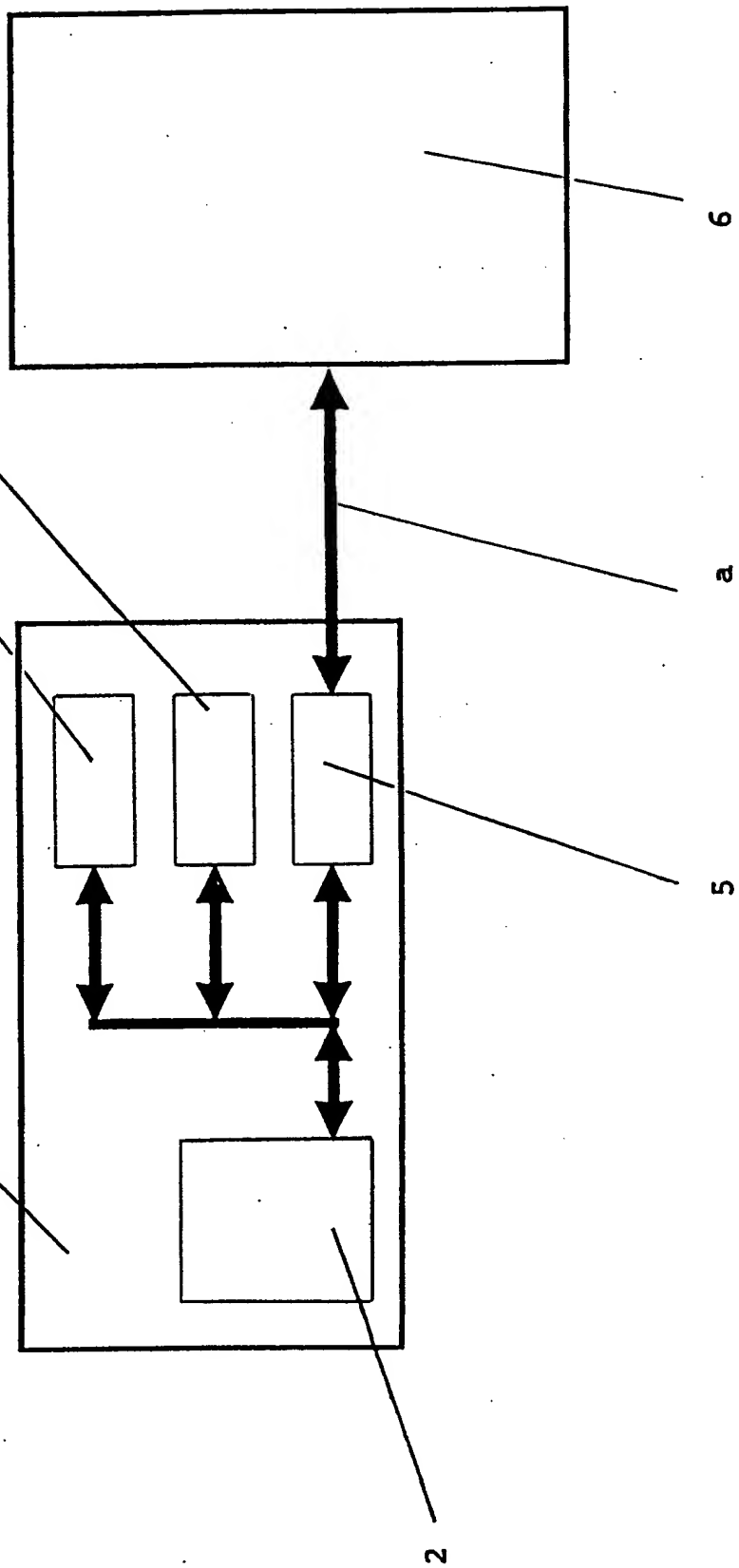
5. Schritt

die digitale Information und mit dem internen Entschlüsselungsalgorithmus (EA) unter Nutzung des Schlüssels (K), welcher nicht außerhalb des -integrierten Schaltkreises-(1) erscheint, von dem Zentralprozessor CPU-(2) nach

NE:=EA (NV, K)

entschlüsselt und von dem -Zentralprozessor CPU-(2) über das Interface (5) ausgegeben wird und dem Empfänger zur Verfügung steht.

HIERZU EINE SEITE ZEICHNUNGEN



Figur 1

INTERNATIONAL SEARCH REPORT

Inte. ɔnal Application No
PCT/DE 95/00738

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	EP,A,0 033 014 (LICENTIA) 5 August 1981 see page 2, line 25 - page 4, line 18 ---	1 2
Y	FR,A,2 681 165 (GEMPLUS) 12 March 1993 see page 1, line 12 - line 23 see page 2, line 6 - line 9 see page 6, line 16 - page 7, line 29 see page 10, line 7 - line 18 ---	1
A	PATENT ABSTRACTS OF JAPAN vol. 7, no. 186 (E-193) 30 May 1983 & JP,A,58 090 849 (NIPPON DENKI) see abstract --- -/--	2

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 September 1995	28. 09. 95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte. ɔnal Application No
PCT/DE 95/00738

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 266 748 (IBM) 11 May 1988 cited in the application see abstract see column 4, line 47 - column 5, line 27 see column 20, line 5 - line 45	1,2

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0033014	05-08-81	DE-A-	3003998	24-09-81
		US-A-	4484025	20-11-84
FR-A-2681165	12-03-93	NONE		
EP-A-0266748	11-05-88	US-A-	4817140	28-03-89
		DE-D-	3751047	23-03-95
		DE-T-	3751047	10-08-95
		EP-A-	0268139	25-05-88
		JP-C-	1667312	29-05-92
		JP-B-	3032813	14-05-91
		JP-A-	63127334	31-05-88
		US-A-	5109413	28-04-92
		JP-C-	1630817	26-12-91
		JP-B-	2060009	14-12-90
		JP-A-	63128434	01-06-88

INTERNATIONALER RECHERCHENBERICHT

Inter nales Aktenzeichen
PCT/DE 95/00738

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6, H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y A	EP,A,0 033 014 (LICENTIA) 5. August 1981 siehe Seite 2, Zeile 25 - Seite 4, Zeile 18	1 2
Y	FR,A,2 681 165 (GEMPLUS) 12. März 1993 siehe Seite 1, Zeile 12 - Zeile 23 siehe Seite 2, Zeile 6 - Zeile 9 siehe Seite 6, Zeile 16 - Seite 7, Zeile 29 siehe Seite 10, Zeile 7 - Zeile 18	1
A	PATENT ABSTRACTS OF JAPAN vol. 7, no. 186 (E-193) 30. Mai 1983 & JP,A,58 090 849 (NIPPON DENKI) siehe Zusammenfassung	2

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
18. September 1995	28.09.95

Name und Postanschrift der Internationale Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Holper, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internes Aktenzeichen
PCT/DE 95/00738

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP-A-0033014	05-08-81	DE-A-	3003998	24-09-81
		US-A-	4484025	20-11-84
FR-A-2681165	12-03-93	KEINE		
EP-A-0266748	11-05-88	US-A-	4817140	28-03-89
		DE-D-	3751047	23-03-95
		DE-T-	3751047	10-08-95
		EP-A-	0268139	25-05-88
		JP-C-	1667312	29-05-92
		JP-B-	3032813	14-05-91
		JP-A-	63127334	31-05-88
		US-A-	5109413	28-04-92
		JP-C-	1630817	26-12-91
		JP-B-	2060009	14-12-90
		JP-A-	63128434	01-06-88